Search Results

Search Results for: **[ssl <AND>(meta_published_date <= 01-01-2000)]**
Found **454** of **1,617 searched out of 126,861.**

Warning: Maximum result set of 200 exceeded. Consider refining.

Search within Results

GO > Advanced Search

> Search Help/Tips

Sort by: **Title** **Publication** **Publication Date** **Score**

Results 1 - 20 of 200 **short listing**

Prev Page 1 2 3 4 5 6 7 8 9 10 Next Page

1 Semantics of query languages for network databases 100%

Kazimierz Subieta

ACM Transactions on Database Systems (TODS) September 1985
Volume 10 Issue 3

Semantics determines the meaning of language constructs; hence it says much more than syntax does about implementing the language. The main purpose of this paper is a formal presentation of the meaning of basic language constructs employed in many database languages (sublanguages). Therefore, stylized query languages SSL (Sample Selection Language) and J (Joins) are introduced, wherein most of the typical entries present in other query languages are collected. The semantics of SSL and J are ...

2 Design verification via simulation and automatic test pattern generation 100%

Hussain Al-Asaad , John P. Hayes

Proceedings of the 1995 IEEE/ACM international conference on Computer-aided design December 1995

We present a simulation-based method for combinational design verification that aims at complete coverage of specified design errors using conventional ATPG tools. The error models used in prior research are examined and reduced to four types: gate substitution errors (GSEs), gate count errors (GCEs), input count errors (ICEs), and wrong input errors (WIEs). Conditions are derived for a gate to be completely testable for GSEs; These conditions lead to small test sets for GSEs. Near-minimal test ...

3 Sticky splines: definition and manipulation of spline structures with maintained topological relations 100%

C. W. A. M. van Overveld , Marie Luce Viaud
ACM Transactions on Graphics (TOG) January 1996
Volume 15 Issue 1

This paper describes an augmentation to the spline concept to account for topological relations between different spline curves. These topological relations include incidence relations, constraining the extremes of spline curves to other spline curves, and also more general geometric relations, for example, involving the tangents of spline curves in their extremes. To maintain these incidence relations, some spline curves may have to be transformed (translated, rotated, scaled), or even def ...

4 Formal module level specifications 99%

B. P. Buckles
Proceedings of the 1977 annual conference January 1977

SSL (Software Specification Language) is part of the growing shift of emphasis in software engineering from the latter software development phases to the earlier ones. The purpose of the language is to aid in the process of decomposing functions into subfunctions or, equivalently, systems into subsystems and modules. A formal description of the syntax and semantics exists which has enabled the construction of an automatic translator. The translator makes a series of nontrivial consistency c ...

5 Internet security: firewalls and beyond 98%

Rolf Oppliger
Communications of the ACM May 1997
Volume 40 Issue 5

6 Securing the commercial Internet 98%

Anish Bhimani
Communications of the ACM June 1996
Volume 39 Issue 6

7 A security architecture for computational grids 98%

Ian Foster , Carl Kesselman , Gene Tsudik , Steven Tuecke
Proceedings of the 5th ACM conference on Computer and communications security November 1998

8 Inductive analysis of the Internet protocol TLS 97%

Lawrence C. Paulson
ACM Transactions on Information and System Security (TISSEC) August 1999
Volume 2 Issue 3

Internet browsers use security protocols to protect sensitive messages. An inductive analysis of TLS (a descendant of SSL 3.0) has been performed using the theorem prover Isabelle. Proofs are based on higher-order logic and make no assumptions concerning beliefs of finiteness. All the obvious security goals can be proved; session resumption appears to be secure even if old session keys are compromised. The proofs suggest minor changes to simplify the analysis. TLS, even at an abs ...

9 High-level design verification of microprocessors via error modeling 97%

D. Van Campenhout , H. Al-Asaad , J. P. Hayes , T. Mudge , R. B. Brown
ACM Transactions on Design Automation of Electronic Systems (TODAES) October 1998
Volume 3 Issue 4

A design verification methodology for microprocessor hardware based on modeling

design errors and generating simulation vectors for the modeled errors via physical fault testing techniques is presented. We have systematically collected design error data from a number of microprocessor design projects. The error data is used to derive error models suitable for design verification testing. A class of basic error models is identified and shown to yield tests that provide good coverage of comm ...

10 DFBT: a design-for-testability method based on balance testing 97%

Krishnendu Chakrabarty , John P. Hayes
Proceedings of the 31st annual conference on Design automation conference June 1994

11 Modular specification of incremental program transformation systems 96%

Alan Carle , Lori Pollock
Proceedings of the 11th international conference on Software engineering May 1989

12 Interview with Sameer Parekh 96%

James T. Dennis
Linux Journal August 1997

13 Why a single parallelization strategy is not enough in knowledge bases 95%

S. Cohen , O. Wolfson
Proceedings of the eighth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems March 1989
We argue that the appropriate parallelization strategy for logic-program evaluation depends on the program being evaluated. Therefore, this paper is concerned with the issues of program-classification, and parallelization-strategies. We propose five parallelization strategies that differ based on the following criteria. Their evaluation cost, the overhead of communication and synchronization among processors, and the programs to which they are applicable. In particular, we start our study w ...

14 RBAC on the Web by smart certificates 95%

Joon S. Park , Ravi Sandhu
Proceedings of the fourth ACM workshop on Role-based access control October 1999

15 Separating key management from file system security 95%

David Mazières , Michael Kaminsky , M. Frans Kaashoek , Emmett Witchel
ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles December 1999
Volume 33 Issue 5
No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

16 Internet printing protocol (IPP) encoding and transport 95%
Carl Kugler , Harry Lewis


StandardView December 1998
Volume 6 Issue 4

17 Characteristics of modern system implementation languages 95%

J. M. Bishop , R. Faria
Proceedings of the 1995 ACM 23rd annual conference on Computer science
February 1995

18 Computer-aided analysis and design of information systems 94%

J. F. Nunamaker , Benn R. Konsynski , Thomas Ho , Carl Singer
Communications of the ACM December 1976
Volume 19 Issue 12
This paper describes the use of computer-aided analysis for the design and development of an integrated financial management system by the Navy Material Command Support Activity (NMCSA). Computer-aided analysis consists of a set of procedures and computer programs specifically designed to aid in the process of applications software design, computer selection and performance evaluation. There are four major components: Problem Statement Language, Problem Statement Analyzer, Generator of Alte ...

19 A unified framework for systematic loop transformations 94%

Lee-Chung Lu
ACM SIGPLAN Notices , Proceedings of the third ACM SIGPLAN symposium on Principles and practice of parallel programming April 1991
Volume 26 Issue 7

20 Personal distributed computing: the Alto and Ethernet hardware 94%

Chuck Thacker
Proceedings of the ACM Conference on The history of personal workstations
January 1986
Between 1972 and 1980, the first distributed personal computing system was built at the Xerox Palo Alto Research Center. The system was composed of a number of Alto workstations connected by an Ethernet local network. It also included servers that provided centralized facilities. This paper describes the development of the hardware that was the basis of the system.

Results 1 - 20 of 200 **short listing**

Prev Page 1 2 3 4 5 6 7 8 9 10 Next Page
